REMARKS

Claims 5, 14, and 23 stand rejected under 35 U.S.C. § 112, first paragraph, for failing to enable a person skilled in the art to which the invention pertains to make and use the invention. As will be shown below, claims 5, 14, and 23 are enabled in Applicants' original specification. Claims 5, 14, and 23 are therefore patentable and should be allowed. Applicants respectfully request reconsideration of claims 5, 14, and 23.

Claims 5-7, 14-16, and 23-25 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that Applicant considers the invention. As will be shown below, the scope of claims 5-7, 14-16, and 23-25 is clear such that the public is informed of the boundaries of what constitutes infringement of the present application. As such, claims 5-7, 14-16, and 23-25 satisfy the definiteness requirement of 35 U.S.C. § 112. Applicants respectfully request reconsideration of claims 5-7, 14-16, and 23-25.

Claims 1-27 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Adams, et al. (U.S. Patent Publication No. 2002/0124053) (hereafter 'Adams'). As will be shown below, Adams does not anticipate controlling access to a computer resource as claimed in the present application. Claims 1-27 are therefore patentable and should be allowed. Applicants respectfully traverse each rejection individually below and request reconsideration of claims 1-27.

Claim Rejections – 35 U.S.C. § 112, First Paragraph

Claims 5, 14, and 23 stand rejected under 35 U.S.C. § 112, first paragraph for failing to comply with the enablement requirement. The Office Action takes the position that the "proxy permission table" is not described in the present application in such a way as to enable one of skill in the art to make or use the invention of claims 5, 14, and 23. Applicant's respectfully note in response, however, that the proxy permission table is described in enabling detail at several reference points in Applicants' original specification including, for example, at page 15, line 26 – page 17, line 12, which states:

> Figure 4 sets forth a flow chart illustrating an exemplary method of determining (108 on Figure 3) that the requesting entity has a proxy permission. The method in Figure 4 includes finding 112 a proxy permission record 160 in a proxy permission table 150 in dependence upon the user identification 106. In this exemplary method, finding 112 a proxy permission record 114 from the proxy permission table 150 is accomplished by searching the proxy permission table for a proxy permission record with a field that contains a proxy user identification 121 that corresponds with the requesting entity's user identification 106. The finding of a proxy permission record that contains a proxy user identification 121 that corresponds with the requesting entity's user identification indicates that the requesting entity has a proxy permission.
>
> A proxy permissions table according to the present invention, may, for example, include the data elements illustrated in Table 2:

Table 2: Proxy Permissions Table

RequesterID	Grantor	Scope	Permissions	Rules
doug	pete	\usr\pete\*.doc	r	\shared\rules\122
brian	pete	\usr\pete\*.exe	e	\shared\rules\125
leslie	stacy	\usr\stacy\newsletter.doc	rw	\shared\rules\129
nancy	stacy	\usr\stacy\*.db	rw	\shared\rules\212

> Table 2 includes a proxy permissions table with a column named "RequesterID" that stores user identifications for requesting entities, a column named "Grantor" that stores identifications of users granting proxy permissions to requesting entities, a column named "Scope" that identifies computer resources to which access is granted through proxy permissions, a column entitled "Permissions" that lists the proxy permission granted to the requesting entity, and a column entitled "Rules" that points to files containing proxy rules for the proxy permissions.
>
> Table 2 depicts the existence of proxy permission for read access granted by a user named "pete" to a user named "doug" for all the word processing files in \usr\pete\ if the rules in \shared\rules\122 are satisfied. Similarly in Table 2, "pete" grants "brian" proxy permission for execute access for all the executables in \usr\pete\ if the rules in \shared\rules\125 are satisfied. "Stacy" grants proxy permissions to "leslie" for read/write access to a

> word processing document having pathname \usr\stacy\newletter.doc if the rules in \shared\rules\129 are satisfied. And "stacy" grants proxy permission to "nancy" for read/write access to all the database files in \usr\stacy\.

That is, Applicants' original specification at page 15, line 26 – page 17, line 12, describes in detail a proxy permission table, how to use a proxy permission table, and provides an enabling example of a proxy permission table. Applicants' original specification at this reference point enables a person of skill in the art to make and use a proxy permission table. A proxy permission table is a table. Any reader of skill in the art understands how to make a table. Moreover, a proxy permission table may be used, as described at this reference point as well as in the claims of the present application, in determining that a requesting entity has a proxy permission including finding a proxy permission record in the proxy permission table. Finding a proxy permission record from the proxy permission table is described at this reference point of Applicants' original specification as being accomplished by searching the proxy permission table for a proxy permission record with a field that contains a proxy user identification. That is, a proxy permission table is used to determine that a requesting entity has a proxy permission. Readers of skill in the art will understand from descriptions of a proxy permission table at this reference point, the claims of the present application, and other reference points of Applicants' original specification how to make and use such a proxy permission table. In fact, Applicants have in this case provided a 35 page application, including 22 pages of text and five drawings, that enables each and every element and limitation of each and every claim in the present application. Because a person of skill in the art could make and use the proxy permission table of claims 5, 14, and 23, the claims satisfy the enablement requirement of the first paragraph of 35 U.S.C. § 112. Applicants respectfully request reconsideration of claims 5, 14, and 23.

The Office Action also takes the position that a proxy permission table as described at Applicants' original specification at paragraph 0038, page 10, line 17 – page 11, line 4, is vague and, as such, is a data structure performing the same function as an access control list. Applicants respectfully submit that a proxy permission table is different than an access control list and although either may alternatively be used in determining that a requesting entity has a proxy permission. Applicants' original specification at paragraph 0038, page 10, line 17 – page 11, line 4, states:

> The following form of chmod command, for example:
>
> ```
> chmod –p <proxy_user_id> -r /global_shared_directory/sysadmin/
> rules /usr/bin/shutdown
> ```
>
> may represent creation of a proxy permission for the user identified by <proxy_user_id> associated with a set of proxy rules located at "/global_shared_directory/sysadmin/rules" granting access permission or authority to access a computer resource. In this example, the computer resource is an executable file identified as "/usr/bin/shutdown." The existence of the proxy permission may be represented in data by an entry on an operating system data structure (in Unix, an 'inode') representing the executable file. The data entry representing the existence of a proxy permission may be a Boolean entry or an asterisk, a numeric, a character, or a short string, as will occur to those of skill in the art. Alternatively, the inode may be left unaltered, and the existence of the proxy permission may be represented in data by an entry in an access control list ("ACL") for the resource, the executable file identified as "/usr/bin/shutdown." Alternatively, both the inode and the ACL for a resource may be left undisturbed, and the existence of a proxy permission may be represented in a totally separate data structure such as a proxy permissions table created for that purpose.

That is, Applicants' original specification at paragraph 0038, page 10, line 17 – page 11, line 4, discloses that a proxy permission may be represented in data by an entry in an access control list or, alternatively, a proxy permission may be represented in a totally separate data structure such as a proxy permissions table. An access control list may include permissions in addition to proxy permissions. A proxy permission table, however, as defined by the limitations of claims themselves is a table including a proxy permission record. Although an access control list, as described in the present application, is not a proxy permission table, either an access control list or a proxy permission table as claimed in the present application may be used to determine that a requesting entity has a proxy permission. As mentioned above, determining that a requesting entity has a proxy permission through use of a proxy permission table is enabled in Applicants' original specification at paragraph 0038, page 10, line 17 – page

11, line 4. An alternative method of determining that a requesting entity has a proxy permission through use of an access control list is described in Applicants' original specification at page at page 19, lines 1-18. Applicants' respectfully submit therefore, that although both an access control list and a proxy permission table may be used in determining that a requesting entity has a proxy permission, an access control list and a proxy permission table are not the same as described in Applicants' original specification. Moreover, as explained above Applicants' original specification fully enables a proxy permission table as recited in claims 5, 14, and 23 and the rejections under 35 U.S.C. § 112, first paragraph should be withdrawn. Applicants respectfully request reconsideration of claims 5, 14, and 23.

Claim Rejections – 35 U.S.C. § 112, Second Paragraph

Claims 5-7, 14-16, and 23-25 stand rejected under 35 U.S.C. § 112, second paragraph as being indefinite for failing to particularly point and distinctly claim the subject matter which Applicants regard as the invention. The Office Action takes the position that "it is unclear whether there is a difference between a proxy permission record and a proxy permission indicator." Applicants respectfully submit that the difference between a proxy permission record and a proxy permission indicator is clear from the limitations of the claims themselves. Claim 5 for example recites a proxy permission record in a proxy permission table. Claim 6 recites a proxy permission indicator in a data structure representing a resource and claim 7 recites a proxy permission indicator in an access control list for the resource. That is, a proxy permission record in only located in an proxy permission table while a proxy permission indicator is not. Furthermore, Applicants original disclosure at page 18, lines 3-5, describes a proxy permission indicator as follows:

> The proxy permission indicator can be any data adapted to represent the existence of a proxy permission, including for example, an integer value, a Boolean flag, a special character such as a asterisk, and so on, as will occur to those of skill in the art

That is, a proxy permission indicator indicates the existence of a proxy permission for a resource. A proxy permission record, however, included more than a mere indication of the existence of a permission. In fact, in the exemplary proxy permissions table of Table 2 above, a proxy permissions record includes an field for a 'RequesterID,' a 'Grantor,' 'Scope,' 'Permissions,' and 'Rules.' Applicants respectfully submit therefore that the difference between a proxy permission indicator and the proxy permission record as claimed in the present application is clear to a person of skill in the art.

The Office Action also takes the position that "it is further unclear of the differences between a proxy permission table, a data structure representing the resource, and an access control list for the resource." Again Applicants respectfully submit that the differences between these claim elements is clear from the language in the claims themselves. A proxy permission table as claimed in claim 5 of the present application, for example, includes a proxy permission record. Neither the data structure representing a resource nor the access control lists recited in the claims includes a proxy permission record. Further, an access control list is not a data structure representing a resource. Instead, an access control list is described at page 12, lines 12-13, as follows:

> An ACL provides precise control over who may access a file or directory and what access rights they have

Because a proxy permission table, an access control list, and a data structure representing a resource are different the rejections under 35 U.S.C. § 112, second paragraph should be withdrawn.

The Office Action also takes the position that claims 5-7, 14-16, and 23-25 are indefinite under 35 U.S.C. § 112, second paragraph because "it is also unclear whether applicant intends to differentiate between the terms reading and finding." MPEP 2173 states:

> The primary purpose of this requirement of definiteness of claim language is to ensure that the scope of the claims is clear so the public is informed of the boundaries of what constitutes infringement of the patent.

Applicants respectfully submit that claims 5-7, 14-16, and 23-25 satisfy 35 U.S.C. § 112, second paragraph because the scope of claims 5-7, 14-16, and 23-25 is clear such that the public is informed of the boundaries of what constitutes infringement of the present application. With regard to the essential inquiry pertaining to the definiteness requirement of 35 U.S.C. § 112, second paragraph, MPEP 2173.02 states:

> Definiteness of claim language must be analyzed, not in a vacuum, but in light of:
>
> (A) The content of the particular application disclosure;
>
> (B) The teachings of the prior art; and
>
> (C) The claim interpretation that would be given by one possessing the ordinary level of skill in the pertinent art at the time the invention was made.

The scope of each of claims 5-7 and their corresponding claims 14-16 and 23-25, is definite such that the public is informed of the boundaries of what constitutes infringement of the patent. The scope of claim 5, including the claim term 'finding,' is clear from the language of the claim which recites:

> 5. The method of claim 1 wherein determining that the requesting entity has a proxy permission further comprises finding, in dependence upon a requesting entity identification, a proxy permission record in a proxy permission table.

Furthermore, the claim term 'finding' as recited in claim 5 is described in one exemplary embodiment at page 15, line 26 – page 16, line 8 of Applicants' original specification as follows:

> Figure 4 sets forth a flow chart illustrating an exemplary method of determining (108 on Figure 3) that the requesting entity has a proxy permission. The method in Figure 4 includes finding 112 a proxy permission record 160 in a proxy permission table 150 in dependence upon the user identification 106. In this exemplary method, finding 112 a

> proxy permission record 114 from the proxy permission table 150 is accomplished by searching the proxy permission table for a proxy permission record with a field that contains a proxy user identification 121 that corresponds with the requesting entity's user identification 106. The finding of a proxy permission record that contains a proxy user identification 121 that corresponds with the requesting entity's user identification indicates that the requesting entity has a proxy permission.

Applicants respectfully submit therefore that the scope of claim 5 when analyzed in light of the content of Applicants' original specification is clear such that the public is informed of the boundaries of what constitutes infringement of the patent. Because the scope of claim 5, including the claim term 'finding,' is clear from the language of the claim and Applicants' original specification, claim 5 satisfies the definiteness requirement under 35 U.S.C. § 112, second paragraph. The rejection of claim 5 and its corresponding claims 14 and 23 should therefore be withdrawn and the claims should be allowed.

Applicants further submit that claims 6 and 7 and corresponding claims 15, 16, 24, and 25 satisfy the definiteness requirement under 35 U.S.C. § 112, second paragraph. The scope of claim 6, including the claim term 'reading,' is clear from the language of the claim which recites:

> 6. The method of claim 5 further comprising reading a proxy permission indicator from a data structure representing the resource.

The scope of claim 7, including the claim term 'reading,' is also clear from the language of the claim which recites:

> 7. The method of claim 5 further comprising reading a proxy permission indicator from an access control list for the resource.

Furthermore, the claim term 'reading' as recited in claims 6 and 7 is described in one exemplary embodiment at page 17, line 14– page 18, line 26 of Applicants' original specification as follows:

> The example of Figure 4 includes two alternative methods (117, 115) of reading proxy permission indicators. The method of Figure 4 includes a first alternative way of reading a proxy permission indicator 146 that is reading 117 a proxy permission indicator from a data structure 128 representing a computer resource 134. In the method of Figure 4, the data structure representing a computer resource depicted is an inode. The use of an inode as a data structure representing a computer resource is not a limitation of the present invention. An inode is a data structure often used in Unix operating systems to represent computer resources. In WindowsNT$_{TM}$ data structures representing computer resources are often implemented as entries in a Master File Table ("MFT"). In MSDOS, a data structure representing a computer resource may be an entry in a File Access Table ("FAT"). The use of any data structure to represent a computer resource, as will occur to those of skill in the art, is well within the scope of the present invention.
>
> In the method of Figure 4, a flag or marker in a field in the inode (or other data structure representing a computer resource) can be a proxy permission indicator 146. The proxy permission indicator can be any data adapted to represent the existence of a proxy permission, including for example, an integer value, a Boolean flag, a special character such as a asterisk, and so on, as will occur to those of skill in the art.
>
> The method of Figure 4 includes a second alternative method of reading a proxy permission indicator that is reading 115 the proxy permission indicator from an ACL 162 for the computer resource. The indication of the existence of a proxy permission in an ACL is the presence in the ACL of an ACE allowing proxy access, such as, for example, an ACE fashioned according to the following structure:

```
struct ACCESS_ALLOWED_PROXY_ACE
{
        ACE_HEADER Header;
        ACCESS_MASK Mask;
        DWORD RequesterID;
        Boolean ProxyPermissionExists;
}
```

> In this example, reading 115 a proxy indication from an ACL may be carried out by scanning through the ACEs of an ACL looking for one that

> allows proxy permissions for a user whose identification matches the contents of ACCESS_ALLOWED_PROXY_ACE.RequesterID. Processing then may proceed by looking up a proxy permission record for the user identified as "RequesterID" in a proxy permission table of the kind illustrated in Table 2.

Applicants respectfully submit therefore that the scope of claims 6 and 7 when analyzed in light of the content of Applicants' original specification is clear such that the public is informed of the boundaries of what constitutes infringement of the patent. Because the scope of claims 6 and 7, including the claim term 'reading,' is clear from the language of the claims and Applicants' original specification, claims 6 and 7 satisfy the definiteness requirement under 35 U.S.C. § 112, second paragraph. The rejection of claims 6 and 7 and corresponding claims 15, 16, 24, and 25 should therefore be withdrawn and the claims should be allowed.

Claim Rejections – 35 U.S.C. § 102 Over Adams

Claims 1-27 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Adams (U.S. Patent No. 2002/0124053). To anticipate claims 1-27 under 35 U.S.C. § 102(b), Adams must disclose each and every element and limitation recited in the claims of the present application. As explained below, Adams does not disclose each and every element and limitation recited in the claims of the present application and therefore does not anticipate the claims of the present application.

Adams Does Not Disclose Each and Every Element Of The Claims Of The Present Application

"A claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). As explained in more detail below, Adams does not disclose each and every element of claim 1, and Adams therefore cannot be said to anticipate the claims of the present application within the meaning of 35 U.S.C. § 102(b).

Independent claim 1 recites:

> 1. A method for controlling access to a computer resource, the method comprising:
>
> receiving from a requesting entity a request for access to the computer resource;
>
> determining that the requesting entity has a proxy permission, wherein the proxy permission has at least one associated proxy rule; and
>
> granting access to the computer resource in dependence upon the proxy rule.

Adams Does Not Disclose Determining That The Requesting Entity Has A Proxy Permission, Wherein The Proxy Permission Has At Least One Associated Proxy Rule

The Office Action takes the position that Adams at paragraphs 0015 and 0017, discloses the second element of claim 1: determining that the requesting entity has a proxy permission, wherein the proxy permission has at least one associated proxy rule. Applicants respectfully note in response, however, that what Adams at paragraph 0015, in fact discloses is:

> [0015] Different access levels may be assigned to each one of the users 110, 112, 114, 116, 118 based on the social network data determined for each user 110, 112, 114, 116, 118. For example, the access levels for a computer file resource 170 (such as a Microsoft Word document, or a hypertext markup language (HTML) file) may include: (1) no access--the user is barred from accessing the resource 170; (2) read-only access--the user can only read the file; (4) read/write access--the user can read and write to the file; (5) execute access--the user can execute (run) the file, or files in a directory; (6) create access--the user can create a new file in a directory; (7) owner access--the user can modify the file, directory, etc.;

> (8) all access--the user has access to all read, write, execute, and create functions to the resource (file) 170; and (9) control access--the user has access to control a remote-controlled device resource 170, including, for example, remotely closing and opening physical doors. However, there may be other access level types as well, such as the ability to change a paper type in a paper tray (e.g., from draft paper to bonded paper) in a shared printer resource 170. For a chat room or bulletin board service application, various access types may include permissions to add, invite, or ban users; permissions to view and/or write posted messages (bulletins); or permissions to run scripts or programs within the chat rooms.

In addition, what Adams at paragraph 0017, in fact discloses is:

> [0017] However, the frequency of communication is but one possible criteria that may be extracted from the social network data to determine access levels. For example, access levels may be granted based on the topics mentioned in the communications between the users 110, 112, 114, 116, 118, 120. That is, the communications may be monitored so as to search for particular keyword(s). Then, access levels may be granted based on the number of occurrences of these particular keyword(s). The various access levels may be granted depending on the number of occurrences (i.e., the more times a specific keyword(s) is found in a communication, the higher level of access is granted). Different weights may be assigned to different keywords, so that certain keywords may have higher weights than others (thus leading to higher access levels). For example, a "point" system may be utilized to keep track of the number of points accumulated based on the occurrence of keywords detected in communications within a period of time. Access levels may also be determined by the user's identity (e.g., certain users are preset to have minimum access levels), the chronology of the communications (e.g., users having more recent communications are granted higher access levels than users having less recent communications), or the resources (such as a particular file, type of file, a Web page, a document, etc.) transmitted to and/or received from the user. Access levels may also be determined by a user's interest in the shared resource 170, such that the greater the interest in the shared resource 170 (e.g., the greater the frequency of accessing the shared resource), the higher access level may be provided over time.

That is, Adams at paragraphs 0015 and 0017, discloses assigning access levels to users based on social network data. Adams' assigning access levels to users based on social network data does not disclose determining that the requesting entity has a proxy permission, wherein the proxy permission has at least one associated proxy rule as claimed in the present application. Adams' access levels do not disclose a proxy permission as claimed in the present application. A proxy permission as claimed in the present application includes at least one associated proxy rule. Adams' access levels, however, include no rules of any sort but instead only identify for a user a level of access to a computer resource. That is, Adams' access levels identify whether a user has no access, read access, read/write access, execute access, create access, and the like. Adams' access levels, not including any rule of any sort, are used to grant or deny access to resources. As claimed in the present application, however, granting access to the computer resource occurs in dependence upon a proxy rule. Because Adams does not disclose a proxy rule as claimed in the present application, Adams does not disclose determining that the requesting entity has a proxy permission, wherein the proxy permission has at least one such associated proxy rule as claimed in the present application. Because Adams does not disclose each and every element and limitation of Applicants' claims, Adams does not anticipate Applicants' claims, and the rejections under 35 U.S.C. § 102(b) should be withdrawn.

Adams Does Not Disclose Granting Access To The Computer Resource In Dependence Upon The Proxy Rule

The Office Action takes the position that Adams at paragraph 17, quoted above, discloses the third element of claim 1: granting access to the computer resource in dependence upon the proxy rule. Applicants respectfully note in response, however, that what Adams at paragraph 0017, in fact discloses is assigning access levels to users based on social network data. Adams' assigning access levels to users based on social network data does not disclose granting access to the computer resource in dependence upon the proxy rule as claimed in the present application because Adams does not disclose a proxy rule as claimed in the present application. Because Adams does not disclose a proxy rule, Adams cannot disclose granting access to a computer resource in dependence upon such proxy rule as claimed here. Because Adams does not disclose each and every element and limitation of Applicants' claims, Adams does not anticipate Applicants' claims, and the rejections under 35 U.S.C. § 102(b) should be withdrawn.

Relations Among Claims

Independent claims 10 and 19 recite system and computer program product claims for controlling access to a computer resource corresponding to independent method claim 1 that include "means for" and "means, recorded on [a] recording medium, for" controlling access to a computer resource.

For the same reasons that Adams does not disclose a method for controlling access to a computer resource, Adams also does not disclose or enable systems and computer program products for controlling access to a computer resource corresponding to independent claims 10 and 19. Independent claims 10 and 19 are therefore patentable and should be allowed.

Claims 2-9, 11-18, and 20-27 depend respectively from independent claims 1, 10, and 19. Each dependent claim includes all of the limitations of the independent claim from which it depends. Because Adams does not disclose or enable each and every element of the independent claims, Adams does not disclose or enable each and every element of the dependent claims of the present application. As such, claims 2-9, 11-18, and 20-27 are also patentable and should be allowed.

Conclusion

Claims 5, 14, and 23 stand rejected under 35 U.S.C. § 112, first paragraph, for failing to enable a person skilled in the art to which the invention pertains to make and use the invention. As explained above, claims 5, 14, and 23 are enabled in Applicants' original specification. Claims 5, 14, and 23 are therefore patentable and should be allowed. Applicants respectfully request reconsideration of claims 5, 14, and 23.

Claims 5-7, 14-16, and 23-25 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter that Applicant considers the invention. As explained above, the scope of claims 5-7, 14-

16, and 23-25 is clear such that the public is informed of the boundaries of what constitutes infringement of the present application. As such, claims 5-7, 14-16, and 23-25 satisfy the definiteness requirement of 35 U.S.C. § 112. Applicants respectfully request reconsideration of claims 5-7, 14-16, and 23-25.

Claims 1-27 stand rejected under 35 U.S.C. § 102 as being anticipated by Adams. Adams does not disclose each and every element of Applicants' claims. Adams therefore does not anticipate Applicants' claims. Claims 1-27 are therefore patentable and should be allowed. Applicants respectfully request reconsideration of claims 1-27.

The Commissioner is hereby authorized to charge or credit Deposit Account No. 09-0447 for any fees required or overpaid.

Respectfully submitted,

Date: November 9, 2007 By: John Biggers

John Biggers
Reg. No. 44,537
Biggers & Ohanian, LLP
P.O. Box 1469
Austin, Texas 78767-1469
Tel. (512) 472-9881
Fax (512) 472-9887
ATTORNEY FOR APPLICANTS